EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

Autor(en): **Archinard, Gabriel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-46902

EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

par Gabriel ARCHINARD

INTRODUCTION

Soit K/k une extension finie de corps de nombres et O_K et O_k leurs anneaux d'entiers. L'existence d'un élément $\theta \in O_K$ tel que $O_K = \mathbf{Z}[\theta]$ — on dit alors que O_K est monogène — facilite grandement l'étude de l'arithmétique de O_K.

Dans une étude récente, J.-J. Payan obtient des conditions nécessaires pour que O_K soit monogène lorsque k est le corps Q ou un corps quadratique imaginaire et lorsque K/k est cyclique de degré premier impair [6].

Dans le cas où $k = Q$, soit n le degré de K/Q, Δ_K le discriminant de K/Q, $\Delta(\theta)$ le discriminant de l'élément $\theta \in O_K$ et $I(\theta)$ son indice $(\Delta(\theta) = (I(\theta))^2 \Delta_K)$. Alors, la conditions $I(\theta) = \pm 1$ est nécessaire et suffisante pour que $O_K = \mathbf{Z}[\theta]$. $I(\theta)$ pouvant s'exprimer comme forme primitive de degré $\frac{1}{2} n(n-1)$ en $n-1$ variables à valeurs entières, [4], la recherche des générateurs de O_K est équivalente à la résolution de l'équation diophantienne $I(\theta) = \pm 1$. Un cas simple où O_K n'est pas monogène est celui où les nombres $I(\theta)$, $\theta \in O_K$, ont un diviseur commun autre que ± 1. Le critère de Hensel [3], permet de déterminer ces cas en considérant la décomposition des nombres premiers inférieurs à n dans O_K, et Nagell, [5], donne des conditions d'existence de diviseurs communs des indices autres que ± 1, pour les extensions cubiques et pour certaines extensions de degré > 4.

Dans ce travail, j'étudie l'existence d'un générateur de l'anneau des entiers dans le cas des extensions K/Q cubiques cycliques, et j'utilise pour ceci la construction due à A. Châtelet ([1], chap. I à IV) dont l'essentiel est rappelé au chapitre 1. Cette construction établit une application de l'ensemble des couples (θ, σ), formés d'un nombre cubique cyclique θ et d'un générateur de $\mathrm{Gal}(Q(\theta)/Q)$, dans $Q(j) \times Z$, où $j = \frac{1}{2}(-1+i\sqrt{3})$. Si $(\beta, S) \in Q(j) \times Z$ est l'image de (θ, σ) par cette application, S est la trace de θ et on dit que θ est construit avec (β, S) et que β engendre $Q(\theta)$ ($Q(\theta)$

ne dépendant pas de S). De plus, toute extension cubique cyclique K/Q est engendrée par un entier de $Q(j)$ dont la norme est produit de nombres premiers distincts et congrus à 1 (mod 3). Un tel entier est dit canonique et permet la construction de bases d'entiers de K dites aussi canoniques.

Dans le chapitre 2, en utilisant une base canonique de K, j'obtiens pour $I(\theta)$ les formes (2.1) et (2.2), ce qui amène notamment à la propriété suivante:

Propriété 2.3 Soit K le corps engendré par l'entier canonique $a_1 j + a_2 j^2$ ($a_i \in Z$). Alors, 2 est diviseur commun des indices de K si et seulement si $a_1 - a_2$ est pair.

Dans le chapitre 3, j'obtiens le résultat principal de ce travail: des conditions nécessaires et suffisantes sur (β, S) pour que le nombre θ construit avec (β, S) soit générateur de l'anneau des entiers de $Q(\theta)$. Ces conditions, trop longues à énoncer dans cette introduction, sont données par le théorème 3.2. On en déduit aisément les théorèmes suivants:

Théorème 3.3 Soit K/Q une extension cubique cyclique de discriminant m^2. Alors, si O_K est monogène, l'équation diophantienne suivante est soluble:

$$X^2 + 3X + 9 = mY^3 .$$

Théorème 3.4 Soit $m \neq 1$, un produit de nombres premiers et congrus à 1 (mod 3). Alors,

a) si l'équation diophantienne

$$X^2 + 3X + 9 = mY^3$$

est soluble, avec $X \not\equiv 0 \pmod 3$ ou $X \equiv 12 \pmod{27}$, il existe une extension cubique cyclique de Q, modérément ramifiée, de discriminant m^2 et dont l'anneau des entiers est monogène.

b) si l'équation diophantienne

$$X^2 + X + 1 = mY^3$$

est soluble, il existe une extension cubique cyclique de Q, sauvagement ramifiée, de discriminant $81\,m^2$ et dont l'anneau des entiers est monogène.

Ces équations présentent l'avantage de se réduire à des équations du deuxième degré en une variable lorsqu'on fixe la valeur de Y. J'ai utilisé

cette méthode en donnant à Y les valeurs de 1 à 100000 et à m une centaine de valeurs pour chacune des équations a) et b).

Les résultats sont exposés aux chapitres 4 (4.1 et 4.2).

Dans un travail récent [2], M.-N. Gras obtient, par d'autres méthodes, des résultats semblables aux théorèmes 3.3 et 3.4 et donne une liste très fournie de corps cubiques cycliques dont l'anneau est soit monogène, soit non monogène.

MM. les professeurs F. Châtelet et J.-J. Payan m'ont dirigé et aidé dans ce travail; je leur exprime ici ma très vive reconnaissance.

Je remercie aussi M. R. Smadja dont un manuscrit m'a été utile dans la recherche des conditions du théorème 3.2 et M^me M. Archinard, qui a bien voulu se charger de la programmation.

Enfin, je remercie le Centre d'économétrie de l'Université de Genève qui m'a donné accès à l'ordinateur de l'Etat de Genève.

Chapitre 1. — Construction des extensions cubiques cycliques de Q

On rappelle dans ce chapitre la construction donnée par A. Châtelet. ([1], chap. 1 à IV).

1. Notations

Dans la suite, K désigne une extension cubique cyclique du corps Q des rationnels, O_K l'anneau des entiers de K, Δ_K le discriminant de K/Q et $\mathrm{Gal}(K/Q)$ son groupe de Galois. E désigne le corps $Q(j)$, où $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, O_E l'anneau des entiers de E, τ le Q-automorphisme de E défini par $\tau j = j^2$ et β' l'élément $\tau\beta$, pour $\beta \in E$. τ désigne aussi le prolongement de τ à $K(j)$ ayant K comme corps des invariants. σ désigne à la fois un élément non trivial de $\mathrm{Gal}(K/Q)$ et son prolongement à $K(j)$ qui laisse E invariant. E est donc le corps des invariants du groupe cyclique engendré par σ.

θ étant un élément de K, on définit les expressions suivantes (résolvantes de Lagrange).

$$<\theta, \sigma> = \theta + j\sigma\theta + j^2\sigma^2\theta \quad \sigma \in \mathrm{Gal}(K/Q)$$

Ce sont des éléments de $K(j)$, qui vérifient les propriétés suivantes:

$$(1.1) \qquad \sigma^l<\theta,\sigma> = <\sigma^l\theta,\sigma> = j^{2l}<\theta,\sigma> \qquad l = 0,1,2.$$
$$\sigma^l<\theta,\sigma^2> = <\sigma^l\theta,\sigma^2> = j^l<\theta,\sigma^2> \qquad l = 0,1,2.$$

$$(1.2) \qquad \tau<\theta,\sigma> = <\theta,\sigma^2>$$

$$(1.3) \qquad \theta = \frac{1}{3}(S + <\theta,\sigma> + <\theta,\sigma^2>)$$

2. Théorèmes fondamentaux

On donne ici les résultats essentiels de la construction de Châtelet et celles de leurs conséquences techniques qui seront utilisées aux chapitres 2 et 3. Pour les démonstrations, on renvoie à [1], en notant que les principales d'entre elles font intervenir de manière systématique les propriétés de $<\theta,\sigma>$ et la théorie de Galois dans $K(j)/Q$.

Lemme 1.1 Soit θ un élément primitif de K. Alors, le nombre β défini par

$$\beta = \frac{<\sigma^l\theta,\sigma>^2}{<\sigma^l\theta,\sigma^2>}$$

est un nombre primitif de E ne dépendant pas de l et vérifiant $\beta^2\,\beta' \notin E^3$.

Si φ est un nombre algébrique engendrant un corps cubique cyclique sur Q et ρ un générateur de $\mathrm{Gal}(Q(\varphi)/Q)$ tels que

$$\frac{<\rho^l\varphi,\rho>^2}{<\rho^l\varphi,\rho^2>} = \beta, \text{ alors } \varphi = \sigma^l\theta - \frac{1}{3}(S-T), \text{ pour } l = 0$$

1 ou 2 et $\rho = \sigma$; S et T étant les traces de θ et φ.

Lemme 1.2 Soit $S \in Q$ et β un nombre primitif de E vérifiant $\beta^2\,\beta' \notin E^3$. Alors, il existe un nombre algébrique θ, de trace S, engendrant une extension cubique cyclique K/Q, et un générateurs σ de $\mathrm{Gal}(K/Q)$ tels que

$$\beta = \frac{<\theta,\sigma>^2}{<\theta,\sigma^2>}.$$

Ces deux lemmes permettent d'énoncer le théorème fondamental de cette construction des corps cubiques cycliques.

Théorème 1.1 Les formules $S = \text{trace}(\theta)$ et

$$\beta = \frac{<\theta, \sigma>^2}{<\theta, \sigma^2>}$$

définissent une surjection de l'ensemble des couples (θ, σ), formés d'un nombre algébrique engendrant un corps cubique cyclique et d'un générateur du groupe de Galois de ce corps, sur l'ensemble des couples (β, S), formés d'un nombre primitif β de E tel que $\beta^2 \beta' \notin E^3$ et d'un nombre rationnel.

Deux couples (θ, σ) et (φ, ρ) ont même image si et seulement si $\varphi = \sigma^l \theta$, pour $l = o$, 1 ou 2 et $\rho = \sigma$.

Définition 1.1 Dans la suite, lorsqu'on se référera à cette construction, on dira que (β, S) est l'image de (θ, σ), que θ est construit avec (β, S) et que β engendre $Q(\theta)$.

Remarque 1.1 Il découle de la définition de $<\theta, \sigma>$ et de la propriété (1.2) que, si (β, S) est l'image de (θ, σ), $(-\beta, -S)$ est l'image de $(-\theta, \sigma)$ et (β', S) celle de (θ, σ^2).

On est ainsi amené à la définition suivante:

Définition 1.2 Soit α et β deux éléments de E. α et β sont dits équivalents si $\alpha \in \{\beta, \beta', -\beta, -\beta'\}$.

Les résultats techniques suivants seront utiles aux chapitres 2 et 3.

Corollaire 1.1 Si θ est construit avec (β, S), θ est zéro du polynôme

$$(1.4) \quad X^3 - SX^2 + \frac{1}{3}(S^2 - \beta\beta')X - \frac{1}{27}(S^3 - 3S\beta\beta' + \beta\beta'(\beta + \beta')).$$

Corollaire 1.2 Soit θ un nombre construit avec (β, S), et soit $\Delta(\theta)$ le discriminant de $1, \theta, \theta^2$ et $\Delta(1, \theta, \sigma\theta)$ celui de $1, \theta, \sigma\theta$. On a alors:

$$(1.5) \quad \Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta - \beta')^2$$

$$(1.6) \quad \Delta(1, \theta, \sigma\theta) = (\beta\beta')^2$$

Corollaire 1.3 Soit (β, S) l'image de (θ, σ). On a alors:

$$(1.7) \quad 9\theta^2 = (\beta + \beta' + 4S)\theta + (j^2\beta + j\beta' - 2S)\sigma\theta + (j\beta + j^2\beta' - 2S)\sigma^2\theta + 2\beta\beta' + S^2$$

$$(1.8) \quad 9\sigma\theta\sigma^2\theta = (\beta + \beta' - 2S)\theta + (j^2\beta + j\beta' + S)\sigma\theta + (j\beta + j^2\beta' + S)\sigma^2\theta - \beta\beta' + S^2$$

Théorème 1.2 Soit (β, S) et (γ, T) les images respectives de (θ, σ) et (φ, ρ). Alors la condition

$$\frac{\gamma^2\gamma'}{\beta^2\beta'} \in E^3$$

est nécessaire et suffisante pour que $Q(\theta) = Q(\varphi)$ et $\sigma = \rho$.

Ce théorème et la remarque 1.1 permettent de reconnaître les nombres engendrant le même corps cubique cyclique.

3. L'ANNEAU O_E

On rappelle d'abord quelques résultats classiques. O_E est intègre, principal et donc factoriel.

$$O_E = Zj \oplus Zj^2 \qquad \text{(somme directe)}$$

Les unités de O_E sont $\pm 1, \pm j, \pm j^2$ et représentent les 6 classes de $O_E/(3)$ premières avec 3.

Les nombres (entiers rationnels) premiers congrus à $-1 \pmod 3$ sont irréductibles dans O_E, les nombres premiers p congrus à 1 (mod 3) sont de la forme $p = \omega_p \omega_p'$, ω_p étant irréductible et ω_p et ω_p' n'étant pas associés. Enfin, on a $3 = -(j - j^2)^2$.

Ainsi, les éléments irréductibles de O_E sont $j - j^2$, les nombres premiers congrus à $-1 \pmod 3$, les éléments ω_p et ω_p' et leurs associés.

Lemme 1.3 Soit β un élément de O_E sans facteurs rationnels et soit p un nombre premier tel que p^n divise exactement $\beta\beta'$. Alors, $p = 3$ et $n = 1$, ou $p \equiv 1 \pmod 3$ et ω_p^n divise exactement β, ω_p étant un diviseur irréductible de p.

Démonstration Si 3^n divise $\beta\beta'$, $j - j^2$ divise exactement β, donc $j - j^2$ divise aussi exactement β' et 3 divise exactement $\beta\beta'$. Il s'ensuit que $n = 1$.

Si $p \neq 3$, p est congru à 1 (mod 3), sinon p serait irréductible et diviserait β. Donc $p = \omega_p \omega_p'$ et ω_p^n et $\omega_p'^n$ divisent exactement $\beta\beta'$. Comme $\omega_p \omega_p'$ ne divise pas β, il faut que ω_p^n (ou $\omega_p'^n$) divise exactement β. C.q.f.d.

Définition 1.3 Un élément de O_E est dit entier canonique s'il n'est divisible ni par $j - j^2$, ni par un entier rationnel, ni par un facteur carré.

Un entier canonique α est de la forme $\omega_{p1} \omega_{p2} \ldots \omega_{pr}$, sa norme étant égale à $p_1 p_2 \ldots p_r$, les p_i étant des nombres premiers naturels distincts et congrus à 1 (mod 3), et satisfait la condition $\alpha^2 \alpha' \notin E^3$.

Réciproquement, un nombre de O_E dont la norme a cette forme est un entier canonique.

Un entier canonique, étant premier avec 3, appartient à l'une des 6 classes de $O_E/(3)$, premières avec 3. Il est donc congru (mod 3) à une unité.

Définition 1.4 Un entier canonique est dit unitaire positif (respectivement négatif) s'il est congru (mod 3) à 1 (respectivement à -1).

Si le signe n'intervient pas, on dit simplement que l'entier canonique est unitaire.

Tour entier canonique est le produit d'une unité et d'un entier canonique unitaire positif unique.

Théorème 1.3 Tout corps cubique cyclique K est engendré par un entier canonique, défini de manière unique à l'équivalence près.

Voir [1], chapitre III, pour une démonstration.

Des entiers canoniques équivalents étant ensemble unitaires ou non, on peut donner la définition suivante:

Définition 1.5 K est dit unitaire s'il est engendré par des entiers canoniques unitaires. (De ces entiers canoniques unitaires, deux sont positifs et deux sont négatifs).

Le théorème suivant donne la construction de bases d'entiers d'un corps K.

Théorème 1.4 Soit K le corps cubique cyclique engendré par l'entier canonique α. Alors:

a) si α est unitaire positif (respectivement négatif) et si θ est construit avec $(\alpha, 1)$ (respectivement avec $(\alpha, -1)$), θ, $\sigma\theta$, et $\sigma^2\theta$ forment une base des entiers de K;

b) si α est non unitaire et si θ est construit avec $(3\alpha, o)$, $1, \theta, \sigma\theta$ forment une base des entiers de K.

Définition 1.6 Ces bases sont dites canoniques et construites avec α.

Corollaire 1.4 On conserve les notations du théorème 1.4. Alors,

a) si K est unitaire, il est modérément ramifié et

$$\Delta_K = (\alpha\alpha')^2$$

b) si K est non unitaire, il est sauvagement ramifié et

$$\Delta_K = 81\,(\alpha\alpha')^2\,.$$

Démonstration Ces formules s'obtiennent immédiatement en prenant les discriminants des bases canoniques par la formule (1.6).

Corollaire 1.5 Soit $p_1, p_2, ..., p_r$, r nombres premiers différents de 1, distincts et congrus à 1 (mod 3). Alors il existe 2^{r-1} corps modérément ramifiés de discriminant $(p_1 p_2 ... p_r)^2$ et 2^r corps sauvagement ramifiés de discriminant $81\,(p_1 p_2 ... p_r)^2$.

Tous les corps cubiques cycliques ont leurs discriminants de cette forme, sauf un corps unique de discriminant 81.

Pour une démonstration du théorème 1.4 et du corollaire 1.5, on se reportera à [1], chapitre IV.

Chapitre 2. — Indice d'un nombre de O_K

L'indice d'un nombre θ d'une extension finie K/Q est le nombre $I(\theta) = \sqrt{\Delta(\theta)/\Delta_K}$, où $\Delta(\theta)$ est le discriminant de θ dans K et Δ_K le discriminant de K (cf. [3], chap. III, § 25 et [5]).

Comme au chapitre 1, K/Q désigne dorénavant une extension cubique cyclique et on va utiliser une base canonique (déf. 1.6) pour calculer l'indice d'un élément quelconque de O_K.

Lemme 2.1 Soit θ un élément primitif d'une base canonique de K. Alors, si $\varphi \in O_K$, il existe un nombre $\psi = X\theta + Y\sigma\theta \in O_K$ tel que $\psi - \varphi \in Z$ et $I(\psi) = I(\varphi)$.

Démonstration On considère le cas où θ est construit avec $(\alpha, 1)$, c'est-à-dire où α est unitaire positif. θ, $\sigma\theta$ et $\sigma^2\theta$ forment une base d'entiers de K, donc $\varphi = X_0\theta + X_1\sigma\theta + X_2\sigma^2\theta$, avec $X_i \in Z$, $i = 1, 2, 3$. Soit $\psi = \varphi - X_2$; alors $I(\psi) = I(\varphi)$ et $\psi = (X_0 - X_2)\theta + (X_1 - X_2)\sigma\theta$, d'après $\theta + \sigma\theta + \sigma^2\theta = 1$. ψ a la forme requise.

Les cas où α est unitaire négatif et où K est non unitaire se démontrent de manière semblable. C.q.f.d.

Donc, pour obtenir les indices de tous les nombres de O_K, il suffit de considérer les nombres de la forme $X\theta + Y\sigma\theta$ où X et Y sont des entiers.

Lemme 2.2 Soit K le corps (modérément ramifié) engendré par l'entier canonique unitaire $\alpha = a_1 j + a_2 j^2$ et soit $\theta, \sigma\theta, \sigma^2\theta$ la base canonique construite avec α. Alors, si $\psi = X\theta + Y\sigma\theta$, $\pm I(\psi)$ est égal à:

$$(2.1) \qquad \frac{a_1 - a_2}{3} X^3 + a_2 X^2 Y - a_1 X Y^2 + \frac{a_1 - a_2}{3} Y^3 .$$

On donne la démarche de la démonstration pour le cas où α est unitaire positif.

θ, $\sigma\,\theta$ et $\sigma^2\,\theta$ formant, dans ce cas, une base des entiers de K, on exprime $\psi^2 = X^2\theta^2 + 2\,X\,Y\,\theta\,\sigma\,\theta + Y^2(\sigma\theta)^2$ comme combinaison linéaire de θ, $\sigma\,\theta$, $\sigma^2\,\theta$ à l'aide des formules (1.7) et (1.8), en tenant compte de $S = \theta + \sigma\,\theta + \sigma^2\,\theta = 1$. 1, ψ et ψ^2 étant exprimés comme combinaisons linéaires de θ, $\sigma\,\theta$ et $\sigma^2\,\theta$, l'indice $\pm\, I(\psi)$ est le déterminant de la matrice des coefficients de ces combinaisons. Le calcul donne le résultat annoncé.

La même technique permet de démontrer le lemme suivant:

Lemme 2.3 Soit K le corps (sauvagement ramifié) engendré par l'entier canonique non unitaire $\alpha = a_1 j + a_2 j^2$ et soit 1, θ, $\sigma\,\theta$ la base canonique construite avec α. Alors, si $\psi = X\,\theta + Y\,\sigma\,\theta$, $\pm\, I(\psi)$ est égal à:

$$(2.2) \qquad (a_1 - a_2)X^3 + 3a_2X^2Y - 3a_1XY^2 + (a_1 - a_2)Y^3\,.$$

De ces lemmes découlent aisément la propriété suivante:

Propriété 2.1 Soit K le corps engendré par l'entier canonique $\alpha = a_1 j + a_2 j^2$ et soit $\theta \neq 1$ un des éléments non nuls d'une base canonique de K. Alors, une condition nécessaire et suffisante pour que $O_K = Z[\theta]$ est

$$(2.3) \qquad a_1 - a_2 = \pm\, 3, \text{ si } K/Q \text{ est modérément ramifiée}$$

$$(2.4) \qquad a_1 - a_2 = \pm\, 1, \text{ si } K/Q \text{ est sauvagement ramifiée.}$$

Remarque 2.1 Des formules (2.1) et (2.2), on déduit aisément des équations diophantiennes qui sont résolubles si et seulement si l'anneau des entiers des corps correspondants sont monogènes.

Définition 2.2 Si un entier divise $I(\varphi)$ pour tous les nombres $\varphi \in O_K$, on dit que c'est un diviseur commun des indices de K, ou un diviseur commun extraordinaire des discriminants de K.

D'après le critère de Hensel ([3], chap. III, § 25), seul 2 peut être diviseur commun des indices d'une extention cubique de Q.

La propriété suivante donne une condition nécessaire et suffisante pour qu'il en soit ainsi dans une extention cubique cyclique de Q.

Propriété 2.2 Soit K le corps engendré par l'entier canonique $\alpha = a_1 j + a_2 j^2$. Alors, 2 est diviseur commun des indices de K si et seulement si $a_1 - a_2$ est pair.

Démonstration D'après les lemmes 2.1, 2.2 et 2.3, l'indice d'un nombre quelconque ψ de O_K est de la forme (2.1) ou (2.2), avec X et Y entiers rationnels.

Ces formes s'écrivent respectivement:

$$I(\psi) = \frac{a_1 - a_2}{3}(X^3 - 3X^2Y + Y^3) + a_1XY(X - Y)$$

et

$$I(\psi) = (a_1 - a_2)(X^3 - 3X^2Y + Y^3) + 3a_1XY(X - Y).$$

On voit que $I(\psi)$ est pair, pour tous X et Y entiers rationnels si et seulement si $a_1 - a_2$ est pair. C.q.f.d.

Exemple 2.1 Soit K le corps engendré par $\alpha = 5j - j^2$. On a $\alpha\alpha' = 31$ et $\alpha - 1 = 6j$, donc α est canonique unitaire et $K = Q(\theta)$, où θ est zéro du polynôme $X^3 - X^2 - 10X + 8$. Les 3 zéros de ce polynôme forment une base canonique de K et $\Delta_K = 31^2$.

La condition du théorème 2.2 étant satisfaite, 2 est diviseur commun des indices de K.

Remarque 2.2 Si 2 est diviseur commun des indices de K, O_K n'est pas monogène; mais on verra, au chapitre 4, qu'il existe des corps K où 2 n'est pas diviseur commun des indices et où O_K n'est pas monogène.

Chapitre 3. — Les nombres cubiques cycliques θ pour lesquels $Z[\theta]$ est l'anneau des entiers de $Q(\theta)$

Soit θ un nombre cubique cyclique construit avec (β, S) (cf. théorème 1.1). On cherche des conditions pour que l'anneau des entiers de $Q(\theta)$ soit $Z[\theta]$.

Lemme 3.1 Soit θ un nombre cubique cyclique, construit avec (β, S), tel que $Z[\theta]$ soit l'anneau des entiers de $Q(\theta)$. Alors $\beta = \frac{b+d}{c}j + \frac{b}{c}j^2$, où d est égal à 1 ou à 3 et où b et c sont des entiers rationnels premiers entre eux.

Démonstration Soit $\beta = b_1 j + b_2 j^2$. b_1 et b_2 sont des nombres rationnels. $1, \theta, \theta^2$ étant une base d'entiers de $Q(\theta)$, on a

$$\frac{\Delta(1, \theta, \sigma\theta)}{\Delta(1, \theta, \theta^2)} \in Z.$$

D'après les formules (1.5) et (1.6), cette condition s'écrit

$$-\frac{27}{(\beta-\beta')^2} \in Z .$$

Mais $(\beta-\beta')^2 = (j-j^2)^2 (b_1-b_2)^2 = -3(b_1-b_2)^2$. La condition s'écrit donc $\dfrac{9}{(b_1-b_2)^2} \in Z$, soit $\dfrac{3}{b_1-b_2} \in Z$.

Soit $b_1 - b_2 = \dfrac{d}{c}$, avec c et d entiers rationnels premiers entre eux et $d > 0$; la condition $\dfrac{3}{b_1-b_2} \in Z$ devient $\dfrac{3c}{d} \in Z$, ce qui implique, c et d étant premiers entre eux et d étant positif, $d = 1$ ou $d = 3$.

Par ailleurs, $\theta \in O_K$ donc $\Delta(1, \theta, \sigma\theta) \in Z$; soit, d'après (1.6) $\beta\beta' \in Z$.

Mais $\beta = \left(b_2 + \dfrac{d}{c}\right) j + b_2 j^2$; donc $\beta\beta' = b_2^2 + b_2 \dfrac{d}{c} + \left(\dfrac{d}{c}\right)^2$.

La condition $\beta\beta' \in Z$ implique, c étant entier, $b_2^2 c^2 + b_2 d c + d^2 \in Z$.

Mais $d \in Z$, donc cette condition s'écrit $b_2^2 c^2 + b_2 d c \in Z$, soit $b_2 c (b_2 c + d) \in Z$. De là on tire $b_2 c \in Z$, soit $b_2 = \dfrac{b}{c}$ avec $b \in Z$.

On a ainsi obtenu $\beta = \dfrac{b+d}{c} j + \dfrac{b}{c} j^2$. C.q.f.d.

Le théorème suivant donne des précisions supplémentaires sur β.

Théorème 3.1 Soit θ un nombre cubique cyclique tel que l'anneau des entiers de $K = Q(\theta)$ soit $Z[\theta]$ et soit (β, S) l'image de (θ, σ). Alors β satisfait l'une des conditions suivantes:

$$(3.1)\quad \begin{cases} \beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2 , \text{ avec } b \in Z , \ b \equiv 1 \pmod 3 , \\ c \in Z \quad \text{et} \quad \left(\dfrac{b^2+b+1}{3c^3}\right)^2 = \Delta_K \end{cases}$$

$$(3.2)\quad \begin{cases} \beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2 , \text{ avec } b \in Z, b \not\equiv 0 \pmod 3 , \\ c \in Z, \ c \not\equiv 0 \pmod 3 \text{ et } \left(\dfrac{b^2+3b+9}{c^3}\right)^2 = \Delta_K \end{cases}$$

$$(3.3)\quad \begin{cases} \beta = \dfrac{3}{c}(b+1)j + \dfrac{3}{c}bj^2, \text{ avec } b \in Z,\ b \not\equiv 1 \pmod 3 \\ \\ c \in Z,\ c \not\equiv 0 \pmod 3 \text{ et } 81\left(\dfrac{b^2+b+1}{c^3}\right)^2 = \Delta_K . \end{cases}$$

Démonstration On obtient ces 3 conditions pour β en prenant successivement, dans la forme de β donnée par le lemme 3.1, $d = 1$, $d = 3$ et $b \not\equiv 0 \pmod 3$ et $d = 3$ et $b \equiv 0 \pmod 3$.

a) $d = 1$

Alors, $\beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2$. L'hypothèse $Z[\theta] = O_K$ entraîne $\Delta(\theta) = \Delta_K$, donc, d'après (1.9), $-\dfrac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \Delta_K$, soit encore $-\dfrac{1}{27}\dfrac{1}{c^6}$ $(b^2+b+1)^2(-3) = \left(\dfrac{b^2+b+1}{3c^3}\right)^2 = \Delta_K$.

Cette condition entraîne $b^2 + b + 1 \equiv 0 \pmod 3$, soit $b \equiv 1 \pmod 3$.

b) $d = 3$ et $b \not\equiv 0 \pmod 3$

c et d étant premiers entre eux, on a $c \not\equiv 0 \pmod 3$.

On a donc $\beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2$, et l'égalité $\Delta(\theta) = \Delta_K$ s'écrit

$$\left(\frac{b^2+3b+9}{c^3}\right)^2 = \Delta_K .$$

c) $d = 3$ et $b \equiv 0 \pmod 3$

Comme en b), on voit que $c \not\equiv 0 \pmod 3$.

En posant $b = 3b_0$, il vient $\beta = \dfrac{3}{c}(b_0+1)j + \dfrac{3}{c} b_0 j^2$.

La condition $\Delta(\theta) = \Delta_K$ s'écrit $81\left(\dfrac{b_0^2+b_0+1}{c^3}\right)^2 = \Delta_K$.

Cette condition ne peut être satisfaite que si $b_0^2 + b_0 + 1 \not\equiv 0 \pmod 3$, c'est-à-dire si $b_0 \not\equiv 1 \pmod 3$. En écrivant b au lieu de b_0, on a les conditions (3.3). C.q.f.d.

Ces conditions (3.1), (3.2) et (3.3) sont deux à deux exclusives.

β étant un nombre satisfaisant l'une de ces conditions et θ étant construit avec (β, S), il se peut, même si S est entier, que θ ne soit pas entier.

Dans les 3 lemmes qui suivent, on donne des conditions pour que θ soit entier, lorsque β satisfait des conditions proches de (3.1), (3.2) ou (3.3).

Pour que θ soit entier, il faut et il suffit que les coefficients du polynôme (1.4) soient entiers, soit que $S \in Z$ et que les 2 conditions suivantes soient satisfaites:

$$\frac{1}{3}(S^2 - \beta\beta') \in Z \tag{3.4}$$

$$\frac{1}{27}(S^3 - 3S\beta\beta' + \beta\beta'(\beta + \beta')) \in Z \tag{3.5}$$

Lemme 3.2 Soit $S \in Z$ et β satisfaisant

$$(3.1)' \quad \begin{cases} \beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z, \\ \\ c \in Z \text{ et } \dfrac{b^2 + b + 1}{3c^3} \in Z. \end{cases}$$

Alors, si θ est construit avec (β, S), une condition nécessaire et suffisante pour que θ soit entier est $S \equiv 0 \pmod 3$ et $b \equiv 4 \pmod 9$.

Démonstration :

$$\beta\beta' = \frac{b^2 + b + 1}{c^2} = 3c \cdot \frac{b^2 + b + 1}{3c^3}$$

est un entier congru à 0 (mod 3), puisque $\dfrac{b^2 + b + 1}{3c^3} \in Z$.

La condition (3.4) est donc équivalente à $S \equiv 0 \pmod 3$, et en tenant compte de ceci, la condition (3.5) est équivalente à $-\dfrac{1}{27}\beta\beta'(\beta + \beta') \in Z$.

Le calcul donne $-\dfrac{1}{27}\beta\beta'(\beta + \beta') = \dfrac{b^2 + b + 1}{27c^3}(2b + 1)$.

Mais $\dfrac{b^2 + b + 1}{3c^3} \in Z$ entraîne $b^2 + b + 1 \equiv 0 \pmod 3$, ce qui est équivalent à $b \equiv 1 \pmod 3$ et à $b^2 + b + 1 \equiv 3 \pmod 9$. Ceci entraîne $c \not\equiv 0 \pmod 3$.

La condition $\dfrac{b^2 + b + 1}{3c^3} \cdot \dfrac{2b + 1}{9} \in Z$ est donc équivalente à $2b + 1 \equiv 0 \pmod 9$, soit à $b \equiv 4 \pmod 9$. C.q.f.d.

Remarque 3.1 La condition $b \equiv 4 \pmod 9$ est équivalente à la condition $\dfrac{b^2 + b + 1}{3c^3} \equiv 7 \pmod 9$ si $c \equiv 1 \pmod 3$ et à la condition $\dfrac{b^2 + b + 1}{3c^3} \equiv -7 \pmod 9$ si $c \equiv -1 \pmod 3$.

Lemme 3.3 Soit $S \in Z$ et β satisfaisant

$$(3.2)' \quad \begin{cases} \beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z, \ b \not\equiv 0 \pmod 3, \\ c \in Z \quad \text{et} \quad \dfrac{b^2 + 3b + 9}{c^3} \in Z. \end{cases}$$

Alors, si θ est construit avec (β, S), une condition nécessaire et suffisante pour que θ soit entier est $S \equiv -bc \pmod 3$.

Démonstration $b \not\equiv 0 \pmod 3$ entraîne $b^2 + 3b + 9 \equiv 1 \pmod 3$. Donc $\dfrac{b^2 + 3b + 9}{c^3} \in Z$ entraîne $c \not\equiv 0 \pmod 3$. Il en résulte $\beta\beta' = \dfrac{b^2 + 3b + 9}{c^2} \equiv 1 \pmod 3$; la condition (3.4) est équivalente à $S \not\equiv 0 \pmod 3$. D'autre part, $\beta\beta'(\beta + \beta') = -\dfrac{b^2 + 3b + 9}{c^3}(2b + 3)$ est entier rationnel et la condition (3.5) entraîne la condition plus faible $S^3 \equiv -\beta\beta'(\beta + \beta') \pmod 3$. D'où, en tenant compte de $S^3 \equiv S \pmod 3$ et de $2b + 3 \equiv -b \pmod 3$, $S \equiv -\dfrac{b^2 + 3b + 9}{c^3} b \pmod 3$.

Mais $\dfrac{b^2 + 3b + 9}{c^3} \equiv c \pmod 3$ puisque $\dfrac{b^2 + 3b + 9}{c^2} \equiv 1 \pmod 3$ et $c \not\equiv 0 \pmod 3$. Il vient $S \equiv -bc \pmod 3$. Réciproquement, on vérifie que si $S \equiv -bc \pmod 3$, la condition (3.5) est satisfaite. C.q.f.d.

Lemme 3.4 Soit $S \in Z$ et β satisfaisant

$$(3.3)' \quad \begin{cases} \beta = \dfrac{3}{c}(b+1) j + \dfrac{3}{c} b j^2, \text{ avec } b \in Z, \ c \in Z \\ \text{et} \quad \dfrac{b^2 + b + 1}{c^3} \in Z \end{cases}$$

Alors, si θ est construit avec (β, S) ,une condition nécessaire et suffisante pour que θ soit entier est $S \equiv 0 \pmod 3$.

Démonstration $\beta\beta' = \frac{9}{c^2}(b^2+b+1)$ est un entier congru à 0 (mod 9), la condition (3.4) est donc équivalente à $S \equiv 0 \pmod 3$. La condition (3.5) est alors aussi satisfaite. En effet $S \equiv 0 \pmod 3$ entraîne $S^3 \equiv 0 \pmod{27}$ et $3 S \beta\beta' \equiv 0 \pmod{27}$. Donc la condition (3.5) est équivalente à $\frac{1}{27}\beta\beta'(\beta+\beta') \in Z$.

Cette dernière condition est vérifiée, car $\beta\beta'(\beta+\beta') = -27 \frac{b^2+b+1}{c^3}(2b+1)$ est un entier congru à 0 (mod 27), puisque $\frac{b^2+b+1}{c^3} \in Z$. C.q.f.d.

Les résultats précédents permettent de démontrer le théorème principal de ce travail:

Théorème 3.2 Soit $(\beta, S) \in E \times Z$ et soit θ construit avec (β, S). Alors $Z[\theta]$ est l'anneau des entiers de $Q(\theta)$ si et seulement si (β, S) satisfait l'une des conditions suivantes:

$$(3.6)\quad \begin{cases} \beta = \dfrac{b+1}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z,\ b \equiv 4 \pmod 9,\ c \in Z \\ \text{et } \dfrac{b^2+b+1}{3c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\ S \equiv 0 \pmod 3 \end{cases}$$

$$(3.7)\quad \begin{cases} \beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2, \text{ avec } b \in Z,\ b \not\equiv 0 \pmod 3,\ c \in Z \\ \text{et } \dfrac{b^2+3b+9}{c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\ S \equiv -bc \pmod 3 \end{cases}$$

$$(3.8)\quad \begin{cases} \beta = \dfrac{3}{c}(b+1) j + \dfrac{3}{c} b j^2, \text{ avec } b \in Z,\ b \not\equiv 1 \pmod 3,\ c \in Z \\ \text{et } \dfrac{b^2+b+1}{c^3} \text{ entier différent de } \pm 1 \text{ et sans facteur carré.} \\ S \equiv 0 \pmod 3 \end{cases}$$

Ces conditions sont deux à deux exclusives et entraînent $\beta\beta'^2 \notin E^3$.

Démonstration Ces conditions sont nécessaires d'après le théorème 3.1 et les lemmes 3.2, 3.3 et 3.4.

D'après ces mêmes lemmes, θ est entier. Il reste donc, pour montrer que ces conditions sont suffisantes, à montrer que dans chacun de ces cas, $\Delta(\theta)$ est le discriminant de $Q(\theta)$.

a) cas où (β, S) satisfait (3.6).

$c\beta = (b+1)j + b j^2$ est sans facteur rationnel. Mais $(c\beta)(c\beta)' = b^2 + b + 1 = 3|c|^3 \dfrac{b^2+b+1}{3|c|^3}$, avec $\dfrac{b^2+b+1}{3|c|^3}$ entier positif distinct de 1 et sans facteurs carrés.

Donc, d'après le lemme 1.3, $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), $\dfrac{b^2+b+1}{3|c|^3}$ est produit de nombres premiers distinct congrus à 1 (mod 3) et $c\beta = (j - j^2)\gamma^3\alpha$, avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \dfrac{b^2+b+1.}{3|c|^3}$

On a de plus $\dfrac{\beta^2\beta'}{\alpha^2\alpha'} = -\left(\dfrac{j-j^2}{c}\right)^3 \gamma^6\gamma'^3 \in E^3$; donc $\beta\beta'^2 \notin E^3$, d'après le théorème 1.2, α engendre $Q(\theta)$.

La formule (1.5) donne $\Delta(\theta) = -\dfrac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \left(\dfrac{b^2+b+1}{3c^3}\right)^2$ $= (\alpha\alpha')^2$; il s'ensuit que $\Delta(\theta) = (\alpha\alpha')^2$ est le discriminant de $Q(\theta)$, d'après le collaire 1.4.

b) Cas où (β, S) satisfait (3.7).

$c\beta = (b+3)j + b j^2$ n'a pas de facteur rationnel, puisque $b \not\equiv 0$ (mod 3). $(c\beta)(c\beta)' = |c^3| \dfrac{b^2+3b+9}{|c|^3}$ avec $\dfrac{b^2+3b+9}{|c|^3} \not\equiv 0 \pmod 3$, différent de 1 et sans facteur carré.

Donc le lemme 1.3 montre que $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), que $\dfrac{b^2+3b+9}{|c|^3}$ est produit de nombres premiers distincts congrus à 1 (mod 3) et que $c\beta = \gamma^3\alpha$ avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \dfrac{b^2+3b+9}{|c|^3}$. Donc $\beta\beta'^2 \notin E^3$.

Le théorème 1.2 montre que α engendre $Q(\theta)$. La formule (1.5) donne $\Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = \left(\frac{b^2+3b+9}{c^3}\right)^2 = (\alpha\alpha')^2$; il s'ensuit que $\Delta(\theta) = (\alpha\alpha')^2$ est le discriminant de $Q(\theta)$, d'après le corollaire 1.4.

c) Cas où (β, S) satisfait (3.8)

$\frac{c}{3}\beta = (b+1)j + bj^2$ n'a pas de facteur rationnel.

$\left(\frac{c}{3}\beta\right)\left(\frac{c}{3}\beta\right)' = |c|^3 \frac{b^2+b+1}{|c|^3}$, avec $\frac{b^2+b+1}{|c|^3} \not\equiv 0 \pmod 3$, différent de 1 et sans facteur carré.

Le lemme 1.3 montre que $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3), que $\frac{b^2+b+1}{|c|^3}$ est produit de nombres premiers distincts et congrus à 1 (mod 3) et que $\frac{c}{3}\beta = \gamma^3\alpha$ avec $\gamma \in O_E$ tel que $\gamma\gamma' = |c|$ et α entier canonique tel que $\alpha\alpha' = \frac{b^2+b+1}{|c|^3}$. Donc $\beta\beta'^2 \notin E^3$ et α engendre $Q(\theta)$ (théorème 1.2). Or $\frac{c}{3}\beta = (b+1)j + bj^2 \not\equiv \pm 1 \pmod 3$ et $\gamma^3 \equiv \pm 1 \pmod 3$, puisque γ est produit d'entiers canoniques, donc congrus à une unité (mod 3). L'égalité $\frac{c}{3}\beta = \gamma^3\alpha$ montre alors que $\alpha \not\equiv \pm 1 \pmod 3$, c'est-à-dire que α est un entier canonique non unitaire.

Il s'ensuit, d'après le corollaire 1.4, que le discriminant de $Q(\theta)$ est $81(\alpha\alpha')^2$.

Et on a ainsi $\Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta-\beta')^2 = 81\left(\frac{b^2+b+1}{c^3}\right)^2 = 81(\alpha\alpha')^2$. C.q.f.d.

Comme sous-produits de la démonstration de ce théorème, on obtient les corollaires suivants:

Corollaire 3.1 Si β satisfait la condition (3.6), $Q(\theta)$ est modérément ramifié, de discriminant $\left(\frac{b^2+b+1}{3c^3}\right)^2$; si β satisfait (3.7), $Q(\theta)$ est modéré-

ment ramifié, de discriminant $\left(\frac{b^2+3b+9}{c^3}\right)^2$; et si β satisfait (3.8), $Q(\theta)$ est sauvagement ramifié, de discriminant $81\left(\frac{b^2+b+1}{c^3}\right)^2$.

Corollaire 3.2 Si β satisfait l'une des conditions (3.6), (3.7), (3.8), $|c|$ est égal à 1 ou est produit de nombres premiers congrus à 1 (mod 3).

Remarque 3.2 Si β satisfait la condition (3.7) (respectivement (3.8)) et si $|c| = 1$, β est entier canonique et satisfait aussi la condition (2.3) (respectivement (2.4)) du théorème 2.1.

C'est le seul cas où l'on peut choisir la trace S de manière que, θ étant construit avec (β, S), 1, θ, θ^2 et θ, $\sigma\theta$, $\sigma^2\theta$ (respectivement 1, θ, $\sigma\theta$) forment des bases d'entiers de $Q(\theta)$.

Définition 3.1 On dit dans ce cas que l'anneau des entiers de $Q(\theta)$ est trivialement monogène.

En abandonnant la référence à (β, S), on peut énoncer:

Théorème 3.3 Soit K/Q une extension cubique cyclique de discriminant $\Delta_K = m^2$. Alors, si O_K est monogène, l'équation diophantienne suivante est soluble:

$$X^2 + 3X + 9 = m\,Y^3 \tag{3.9}$$

Démonstration On garde les notations du théorème 3.2. O_K étant monogène, il existe $\theta \in O_K$, construit avec un couple (β, S) qui satisfait l'une des conditions (3.6), (3.7) ou (3.8).

Si (3.6) est satisfaite, $b^2 + b + 1 = m\,3\,|c|^3$, donc l'équation (3.9) admet la solution $(3b, 3|c|)$.

Si (3.7) est satisfaite, $b^2 + 3b + 9 = m|c|^3$, donc (3.9) admet la solution $(b, |c|)$,

Si (3.8) est satisfaite, $9(b^2+b+1) = m|c|^3$, donc (3.9) admet la solution $(3b, |c|)$.

Ce théorème admet le réciproque suivant:

Théorème 3.4 Soit $m \neq 1$ un produit de nombres premiers distincts et congrus à 1 (mod 3).

Alors:

a) si l'équation diophantienne

(3.10) $$X^2 + 3X + 9 = mY^3$$

est soluble avec $X \not\equiv 0 \pmod 3$ ou avec $X \equiv 12 \pmod{27}$, il existe une extension K/Q modérément ramifiée, de discriminant m^2 et dont l'anneau des entiers est monogène.

b) si l'équation diophantienne

(3.11) $$X^2 + X + 1 = mY^3$$

est soluble, il existe une extension K/Q sauvagement ramifiée, de discriminant $81\,m^2$ et dont l'anneau des entiers est monogène.

Démonstration

a) Si (b, c) est une solution de (3.10) avec $b \not\equiv 0 \pmod 3$ le nombre $\beta = \dfrac{b+3}{c} j + \dfrac{b}{c} j^2$ satisfait la condition (3.7) du théorème 3.2. Ce théorème montre que le nombre θ construit avec $(\beta, -bc)$ engendre un corps K tel que $O_K = Z\ [\theta]$ et $\Delta_K = m^2$.

Si (b, c) est une solution de (3.10) avec $b \equiv 12 \pmod{27}$, alors $b_0 = \dfrac{b}{3}$ est un entier congru à 4 (mod 9) et $c_0 = \dfrac{c}{3}$ est entier. Le nombre $\dfrac{b_0 + 1}{c_0} j + \dfrac{b_0}{c_0} j^2$ satisfait la condition (3.6) du théorème 3.2; ce qui montre que le nombre θ construit avec $(\beta, 0)$ engendre un corps K tel que $O_K = Z\ [\theta]$ et $\Delta_K = m^2$.

b) Soit (b, c) une solution de (3.11). Il faut $b \not\equiv 1 \pmod 3$ et $c \not\equiv 0 \pmod 3$. Le nombre $\beta = 3\dfrac{b+1}{c} j + 3\dfrac{b}{c} j^2$ satisfait la condition (3.8) du théorème 3.2; ce qui montre que le nombre θ construit avec $(\beta, 0)$ engendre un corps K tel que $O_K = Z\ [\theta]$ et $\Delta_K = 81\,m^2$. C.q.f.d.

Remarque 3.3 Si (X, Y) est solution de l'équation diophantienne (3.10), la condition $X \equiv 12 \pmod{27}$ est équivalente à la condition $m \equiv 7 \pmod 9$.

Chapitre 4. — Exemples numériques

Dans ce chapitre, m est le produit de $r \geqslant 1$ nombres premiers distincts et congrus à 1 modulo 3.

Note. En plus des critères obtenus aux chapitres 2 et 3, on utilise, pour étoffer la liste des résultats, un critère donné par Payan dans [6] (proposition 1).

Soit $m = p_1 p_2 \ldots p_r$ la décomposition de m en facteurs premiers. On sait que si K/Q est modérément ramifiée de discriminant m^2 (resp. sauvagement ramifiée de discriminant $81\, m^2$), K est le corps de rupture de $X^3 - 3\,m\,X - a\,m$, avec $4\,m = a^2 + 27\,b^2$ et $a \equiv 1 \pmod 3$ (resp. avec $4\,m = a^2 + 3\,b^2$, $a \equiv 1 \pmod 3$ et $b \not\equiv 0 \pmod 3$). Le critère s'énonce alors ainsi:

Pour que O_K soit monogène, il faut $a^{\frac{p_i - 1}{3}} \equiv 1 \pmod{p_i}$ pour $i = 2, 3, \ldots r$ si K/Q est modérément ramifiée et $(3a)^{\frac{p_i - 1}{3}} \equiv 1 \pmod{p_i}$ pour $i = 1, 2, \ldots r$ si K/Q est sauvagement ramifiée.

1. Les corps modérément ramifiés

Parmi les 4 entiers canoniques unitaires équivalents engendrant un corps modérément ramifié, on choisit l'entier canonique unitaire positif $\alpha = a_1 j + a_2 j^2$ (donc avec $a_1 \equiv a_2 \equiv -1 \pmod 3$) tel que $|a_1| > |a_2|$. On associe ainsi à chaque corps modérément ramifié un entier canonique unique α et réciproquement.

Si $\alpha = (a+1)\,j - a\,j^2$ (avec $a \equiv 1 \pmod 3$), on a $m = 3\,a^2 + 3\,a + 1$, et l'équation (3.10) admet, pour cette valeur de m, la solution $X = 9\,a + 3$ et $Y = 3$, X étant congru à 12 (mod 27). Le nombre θ, construit avec $(\beta, 0)$, où $\beta = (3a+2)\,j + (3a+1)\,j^2$, engendre un corps dont l'anneau des entiers est $Z[\theta]$ (théorème 3.4).

Comme $\dfrac{\beta'^2\beta}{\alpha^2\alpha'} = (j^2 - j)^3$, α engendre aussi le corps $Q(\theta)$. On dit, dans ce cas, que O_K est presque trivialement monogène. Le polynôme irréductible de θ est $X^3 - mX + \dfrac{m}{3}(2a+1)$.

Remarque 4.1 Si O_K est trivialement (resp. presque trivialement) monogène (définition 3.1), on a $4m = a^2 + 27$ (resp. $4m = 1+27b^2$) et inversement. Ces cas sont signalés dans [6].

Pour chaque nombre $m < 2000$, on a calculé les entiers canoniques associés aux 2^{r-1} corps modérément ramifiés de discriminants m^2 (cf. corollaire 1.5).

Si pour un nombre m, l'un de ces entiers canoniques ne satisfait pas l'une des conditions permettant de dire que l'anneau des entiers du corps qu'il engendre admet 2 comme diviseur commun des indices (propriété 2.2), ou qu'il est trivialement ou presque trivialement monogène, on a cherché les solutions (X, Y) de l'équation (3.10), avec $X > 0$ et $0 < Y < 300\,000$ pour $m < 853$ et $0 < Y < 30000$ pour $853 < m < 2000$. Pour chaque solution obtenue, on a calculé le polynôme irréductible du nombre φ construit avec (β, S), où $\beta = \dfrac{X+3}{Y} j + \dfrac{X}{Y} j^2$ et où $S = \pm 1$ et $S \equiv -XY \pmod 3$ si $X \not\equiv 0 \pmod 3$ et où $S = 0$ si $X \equiv 0 \pmod 3$; φ est donc un générateur de l'anneau des entiers de $Q(\varphi)$. On a, ensuite, cherché le générateur canonique α du corps $Q(\varphi)$.

Les résultats sont les suivants:

m	X	Y	Irr (φ)	α
241	286	7	$X^3+X^2-562X+4945$	$-16j-j^2$
373	1598	19	$X^3-X^2-2362X+44981$	$17j-4j^2$
379	911	13	$X^3-X^2-1642X+26165$	$-22j-7j^2$
463	397	7	$X^3+X^2-1080X+13307$	$-22j-j^2$
751	1283	13	$X^3-X^2-3254X+72541$	$-31j-10j^2$
1159	629	7	$X^3-X^2-2704X+55031$	$35j+2j^2$
1213	7837	37	$X^3+X^2-14960X+699317$	$-28j+11j^2$
1321	506370	579	$X^3-254953X+49549389$	$-40j-31j^2$
1381	12745	49	$X^3+X^2-22556X+1296401$	$35j-4j^2$
1603	740	7	$X^3-X^2-3740X+89293$	$41j+2j^2$

Si m est un nombre premier, il n'y a qu'un corps de discriminant m^2 et α est défini par m. C'est le cas pour tous les nombres m de ce tableau sauf pour $1159 = 19 \cdot 61$ et $1603 = 7 \cdot 229$.

Les 2 corps de discriminants 1159^2 sont engendrés respectivement par $-37j - 7j^2$ et $35j + 2j^2$. Le corps engendré par $-37j - 7j^2$ ayant 2 comme diviseur commun des indices, c'est le corps engendré par $35j + 2j^2$ dont l'anneau des entiers est monogène, de générateur φ.

Les 2 corps de discriminants 1603^2 sont engendrés respectivement par $\alpha = 41\,j + 2\,j^2$ et $-46\,j - 19\,j^2$. Or φ est construit avec $\beta = \frac{743}{7}j + \frac{740}{7}j^2$ et on a $\frac{\beta^2\beta'}{\alpha^2\alpha'} = (-2j-3j^2)^3$; c'est donc le corps engendré par α dont l'anneau des entiers est monogène de générateur φ (théorème 1.2).

On donne dans le tableau suivant, pour chaque corps de discriminant $< 1000^2$, la racine carrée du discriminant, les valeurs a_1 et a_2 ($a_1 j + a_2 j^2$ étant l'entier canonique qui engendre le corps) et, si possible, la nature de son anneau des entiers: triv. mon. signifie que l'anneau est trivialement monogène, p. tr. mon. qu'il est presque trivialement monogène, 2 d. c. i. que 2 est diviseur commun des indices (l'anneau n'est donc pas monogène) et, si pour d'autres corps, le critère de Payan (cf. note en début de chapitre) permet d'affirmer que l'anneau n'est pas monogène, on donne la valeur de a correspondante ($4m = a^2 + 27b^2$). La correspondance entre $\alpha = a_1 j + a_2 j^2$ et a se fait en comparant le polynôme du nombre construit avec $(3\alpha, 0)$ (formule 1.4) et le polynôme $X^3 - 3mX - am$.

Pour 34 des 128 corps de ce tableau, les méthodes utilisées n'ont pas permis de déterminer la nature de l'anneau, si ce n'est que cet anneau n'est ni trivialement ni presque trivialement monogène et que 2 n'est pas d. c. i.

m	a_1, a_2	Anneau	m	a_1, a_2	Anneau
7	2, −1	triv. mon.	157	−13, −1	2 d. c. i.
13	−4, −1	triv. mon.	163	14, 11	triv. mon.
19	5, 2	triv. mon.	181	11, −4	?
31	5, −1	2 d. c. i.	193	−16, −7	?
37	−7, −4	triv. mon.	199	−13, 2	?
43	−7, −1	2 d. c. i.	211	14, −1	?
61	5, −4	p. tr. mon.	217=7·31	−16, −13	triv. mon.
67	−7, 2	?	217	17, 8	$a=25$
73	8, −1	?	223	17, 11	2 d. c. i.
79	−10, −7	triv. mon.	229	17, 5	2 d. c. i.
91=7·13	11, 5	2 d. c. i.	241	−16, −1	monogène
91	−10, −1	$a=-11$	247=13·19	17, 14	triv. mon.
97	11, 8	triv. mon.	247	11, −7	2 d. c. i.
103	11, 2	?	259=7·37	−13, 5	2 d. c. i.
109	−7, 5	2 d. c. i.	259	17, 2	$a=19$
127	−13, −7	2 d. c. i.	271	−19, −10	?
133=7·19	11, −1	2 d. c. i.	277	−19, −7	2 d. c. i.
133	−13, −4	$a=-17$	283	−19, −13	2 d. c. i.
139	−13, −10	triv. mon.	301=7·43	20, 11	$a=31$
151	14, 5	?	301	−19, −4	$a=-23$

m	a_1, a_2	Anneau	m	a_1, a_2	Anneau
307	17, −1	2 d. c. i.	661	29, 20	?
313	−19, −16	triv. mon.	673	29, 8	?
331	11, −10	p. tr. mon.	679 = 7·97	17, −13	2 d. c. i.
337	−13, 8	?	679	−25, 2	$a = -23$
349	20, 17	triv. mon.	691	−19, 11	2 d. c. i.
367	−22, −13	?	703 = 19·37	29, 23	2 d. c. i.
373	17, −4	monogène	703	26, −1	$a = 25$
379	−22, −7	monogène	709	−28, −25	triv. mon.
397	23, 11	2 d. c. i.	721 = 7·103	29, 5	2 d. c. i.
403 = 13·31	23, 14	$a = 37$	721	−31, −16	$a = -47$
403	−19, 2	$a = -17$	727	−31, −13	2 d. c. i.
409	23, 8	?	733	−31, −19	2 d. c. i.
421	20, −1	?	739	23, −7	2 d. c. i.
427 = 7·61	−22, −19	triv. mon.	751	−31, −10	monogène
427	23, 17	2 d. c. i.	757	−28, −1	?
433	−13, 11	2 d. c. i.	763 = 7·109	29, 26	triv. mon.
439	23, 5	2 d. c. i.	763	−31, −22	$a = -53$
457	17, −7	2 d. c. i.	769	32, 17	?
463	−22, −1	monogène	787	29, 2	?
469 = 7·67	23, 20	triv. mon.	793 = 13·61	−31, −7	2 d. c. i.
469	−25, −13	2 d. c. i.	793	32, 11	$a = 43$
481 = 13·37	−25, −16	$a = -41$	811	−31, −25	2 d. c. i.
481 = 13·37	−19, 5	2 d. c. i.	817 = 19·43	17, −16	p. tr. mon.
487	23, 2	?	817	32, 23	$a = 55$
499	−25, −7	2 d. c. i.	823	−19, 14	?
511 = 7·73	26, 11	$a = 37$	829	20, −13	?
511	−25, −19	2 d. c. i.	853	−31, −4	?
523	26, 17	?	859	23, −10	?
541	−25, −4	?	871 = 13·67	29, −1	2 d. c. i.
547	14, −13	p. tr. mon.	871	−34, −19	?
553 = 7·79	23, −1	2 d. c. i.	877	−31, −28	triv. mon.
553	−16, 11	$a = -5$	883	−34, −13	?
559 = 13·43	−25, −22	triv. mon.	889 = 7·127	32, 5	$a = 37$
559	17, −10	$a = 7$	889	−25, 8	$a = -17$
571	26, 5	?	907	26, −7	?
577	−19, 8	?	919	35, 17	2 d. c. i.
589 = 19·31	20, −7	$a = 13$	937	32, 29	triv. mon.
589	−28, −13	$a = -41$	949 = 13·73	−28, 5	$a = -23$
601	−25, −1	2 d. c. i.	949	35, 23	2 d. c. i.
607	26, 23	triv. mon.	967	−34, −7	?
613	−28, −19	?	973 = 7·139	29, −4	$a = 25$
619	−22, 5	?	973	−19, 17	2 d. c. i.
631	29, 14	?	991	35, 26	?
643	29, 11	2 d. c. i.	997	23, −13	2 d. c. i.

2. Les corps sauvagement ramifiés

A chaque entier canonique unitaire β correspondent deux entiers canoniques non unitaires, non équivalents, $j\beta$ et $j^2\beta$, et chaque classe d'équivalence d'entiers canoniques non unitaires a un représentant unique de cette forme. On associe ainsi à chaque corps sauvagement ramifié un entier canonique unique α qui l'engendre et réciproquement.

Remarque 4.2 Si O_K est trivialement monogène (définition 3.1), on a $4m = a^2 + 3$ et inversement. Le cas est signalé dans [6].

Pour chaque nombre $m < 2000$, on a calculé les entiers canoniques associés aux 2^r corps sauvagement ramifiés de discriminant $81\,m^2$ (r est le nombre de facteurs premiers de m; cf. corollaire 1.5). Si pour un nombre m, l'un de ces entiers canoniques ne satisfait pas l'une des conditions permettant de dire que l'anneau des entiers du corps qu'il engendre admet 2 comme diviseur commun des indices ou qu'il est trivialement monogène, on a cherché les solutions (X, Y) de l'équation (3.11) avec $0 < X$ et $0 < Y < 301000$ pour $m \leqslant 511$ et $0 < Y < 31000$ pour $511 < m < 2000$. Pour chaque solution obtenue, on a calculé le polynôme irréductible du nombre φ construit avec $(\beta, 0)$, où $\beta = 3\dfrac{X+1}{Y}j + 3\dfrac{X}{Y}j^2$; φ est donc un générateur de l'anneau des entiers de $Q(\varphi)$. On a ensuite cherché l'entier canonique α associé à $Q(\varphi)$. (Cf. théorème 1.2).

Les résultats sont les suivants:

m	X	Y	Irr (φ)	α
307	324	7	$X^3-6447X+199243$	$j+18j^2$
613	1160	13	$X^3-23907X+1422773$	$9j+28j^2$
1159	2819	19	$X^3-66063X+6535601$	$7j-30j^2$
1327	6287	31	$X^3-123411X+16687025$	$-42j-23j^2$
1447	704	7	$X^3-30387X+2038823$	$-2j-39j^2$

Une table analogue à celle qui a été dressée pour les corps modérément ramifiés laisserait apparaître, parmi les 257 corps sauvagement ramifiés de discriminant $< 81^2 \cdot 1000^2$, 19 corps d'anneau trivialement monogène, 2 d'anneau monogène (nontrivial), 88 ayant 2 comme d. c. i., 130 ayant

un anneau non monogène et où 2 n'est pas d. c. i. et 18 dont on n'a pas déterminé la nature de l'anneau, sinon qu'il n'est pas trivialement monogène et que 2 n'est pas d. c. i.

M^me M.-N. Gras, dans une étude sur le même problème [2], obtient, grâce notamment à un critère supplémentaire, des résultats plus nombreux et plus complets. On renvoie à ce travail pour des tables plus fournies.

BIBLIOGRAPHIE

[1] CHATELET, A. Arithmétique des corps abéliens du troisième degré. *Annales E.N.S. (3), LXIII*, fasc. 2 (1946).

[2] GRAS, M.-N. Sur les corps cubiques cycliques dont l'anneau des entiers est monogène. *Annales scientifiques de l'Université de Besançon, 3^e série, fasc. 6* (1973).

[3] HASSE, H. *Zahlentheorie*. Akademie-Verlag, Berlin, 1963.

[4] NAGELL, T. Sur les discriminants des nombres algébriques. *Arkiv för Matematik, 7*, 19 (1967).

[5] —— Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique. *Arkiv för Matematik, 6*, 15 (1965).

[6] PAYAN, J. J. Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur Q ou sur un corps quadratique imaginaire. *Arkiv för Matematik, 11*, 2 (1973).

(Reçu le 27 décembre 1973)

G. Archinard

1, chemin de l'Escalade
CH-1206 — Genève